DOC IT Security Evaluation Checklist: System/Network Administrator Responsibilities

A System/Network Administrator is a DOC federal employee or contractor who operates systems or networks and implements security as directed by the system owner. This checklist provides system/network administrators with a self-assessment tool, and their supervisors or Contracting Officer's Technical Representatives with a performance evaluation tool, to evaluate the level of compliance with system/network administrator's duties as established by the

- *DOC IT Security Program Policy and Minimum Implementation Standards* (ITSPP),
- *DOC Remote Access Policy and Minimum Implementation Standards* (RASP), and
- *DOC Policy on Password Management* (PPM).

This is an assessment of (name/operating unit/office)**:**		
	Self Assessment	**Assessment Date:**
	Third Party Evaluation	**Assessor** (name/title/org.):

Status Codes: **1** = Not Started **2** = In Process **3** = In Place

Performance Levels:

1 System/network administrator is aware of comprehensive IT security policies in place

2 System/network administrator is aware of comprehensive IT security policies as well as detailed procedures in place

3 System/network administrator is familiar with comprehensive IT security policies and detailed procedures in place and fully implements them for the system

4 System/network administrator is familiar with comprehensive IT security policies and detailed procedures in place, fully implements them for the system, and tests them for effectiveness

5 System/network administrator is familiar with, and fully implements and tests, comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

	System/Network Administrator Responsibilities	**DOC Policy References**	**Status**	**Performance Level**
1	Assist system owners in the development and maintenance of security plans and contingency plans for all general support systems and major applications under their responsibility.	ITSPP 2.1.11 and 1(a)-(c)		
	(a) Assist in developing system security plans;	ITSPP 3.5.2		
	(b) Assist in developing and testing contingency plans; and	ITSPP 3.9.2		
	(c) Assist in developing and maintaining system documentation (e.g., hardware, software, and user manuals).	ITSPP 3.12.1, 3.12.2		
2	Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.	ITSPP 3.1.2		
3	Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system, including:	ITSPP 2.1.11 and 3(a)-(d)		
	(a) Assist with the annual security system self-assessment conducted in accordance with NIST SP 800-26;	ITSPP 3.2.1.2		
	(b) Contribute in developing corrective action plans/plans of action and milestones (POAMs);	ITSPP 3.2.1.5		
	(c) Assist with system vulnerability testing; and	ITSPP 3.2.2		
	(d) Participate in the certification and accreditation process.	ITSPP 3.41.2		
4	Evaluate proposed technical security controls and contribute to development of procedures that ensure proper integration with other	ITSPP 2.1.11, 3.3.1, 3.9.2,3.11.2, 3.15.2,		

	System/Network Administrator Responsibilities	DOC Policy References	Status	Performance Level
	system operations.	3.16.1, 3.16.4		
5	Assist the system owner in the identification resources needed to effectively implement and ensure the integrity of technical security controls.	ITSPP 2.1.11, 3.14.11, 3.15.2, 3.16.1.2, 3.16.4.4		
6	Report all incidents to the appropriate Computer Incident Response Capability (CIRC) or Computer Incident Response Team (CIRT) in a timely manner.	ITSPP 2.1.11, 3.14.3, RASP		
7	As directed by the system owner, ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)	ITSPP 2.0.1, RASP, PPM		
8	Read and understand all applicable training and awareness materials.	ITSPP 2.1.11, PPM, RASP		
9	Read and understand all applicable use policies or other rules of behavior regarding use or abuse of operating unit IT resources.	ITSPP 2.1.11, RASP, PPM		
10	Assist the system owner in the development of system administration and operational procedures and manuals.	ITSPP 2.1.11, 3.11.2, RASP, PPM		
11	Know which systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, etc.).	ITSPP 2.1.11		
12	Know the sensitivity of the data they handle and take appropriate measures to protect it.	ITSPP 3.3.1.5		
13	Know and abide by all applicable DOC and operating unit policies and procedures.	ITSPP 1.2, RASP, PPM		
14	Manages changes to firewalls as directed by the Network Manager (system owner), when firewalls in parallel are implemented.	ITSPP 3.16.4.5		
15	Assist in creating firewall policies including minimum standards for firewall configuration and management.	ITSPP 3.16.4.4		
16	Know restrictions established by the Electronic Communications Privacy Act of 1986, with respect to legal issues surrounding the interception of certain communications and other forms of employee surveillance.	ITSPP 3.17.3		
17	Establish procedures for implementing and supporting secure remote access services for authorized remote users, including:	RASP		
	(a)Ensure appropriate security controls on remotely accessible systems are set in accordance with the system security plan for the system to which remote access is allowed.	RASP		
	(b)Follow procedures established for configuring and maintaining approved remote access security technologies (for example, Virtual Private Network servers).	RASP		
	(c) Install system software patches, including anti-virus software signature files, on DOC-owned computers used for remote access as directed by the system owner or ITSO.	RASP		
	(d)Terminate remote access privileges within one business day of notification by the manager, supervisor, or COTR that the privileges must be withdrawn.	RASP		